Doc. Ing. Ladislav Hudec, CSc., Ústav počítačového inžinierstva a aplikovanej informatiky,
Fakulta informatiky a informačných technológií STU, Mlynská dolina, SK-842 16 Bratislava

---

Oponentský posudok dizertačnej práce

Dizertant: Ing. Lukáš Aron, Fakulta informačních technologií, Vysoké učení technické v Brně
Názov práce: Ochrana citlivých informací na mobilních zařízeních (Privacy protection on mobile devices)

Mobilné zariadenia predstavujú významný a užitočný nástroj každodenného života. Vzhľadom na potenciálny výpočtový výkon a dostupnú konektivitu umožňujú mobilné zariadenia používateľom prístup k veľkému množstvu rôznych služieb. Mobilné zariadenia na druhej strane uchovávajú citlivé privátne používateľské údaje, ktoré sa môžu stať lukratívnym cieľom útočníkov. Dizertácia sa zaoberá problematikou ochrany privátnych údajov na mobilnom zariadení. Téma dizertácie je vysoko aktuálna a spadá do odboru Výpočtová technika a informatika.

Predložená dizertačná práca je nadštandardného rozsahu. Obsahuje 10 kapitol, tri prílohy a 247 citovaných zdrojov. Celkovo má 177 strán.

Pôvodným prínosom dizertačnej práce je navrhnutie nového formálneho modelu riadenia prístupu k súborom na mobilnom zariadení. Doterajšie prístupy poskytujúce podobnú ochranu privátnosti vychádzali zo statického stavu a implementácia ochrany privátnosti predpokladala modifikáciu operačného systému. Nový formálny model špecifikuje vyžadované správanie a môže byť použitý na účely verifikácie. Navrhnutý model vyžadovaného správania je rozdelený na dve časti. Prvá časť je vyjadrená deterministickým konečno stavovým automatom, ktorý reprezentuje akcie vykonané so súbormi z pohľadu používateľa alebo aplikácie. Prechodová funkcia automatu je definovaná prostredníctvom operácií so súbormi. Druhá časť nového formálneho modelu je vysokoúrovňový pohľad na možné prechody súborov. Aby bolo možné uchopiť dynamicky sa meniace prostredie, v ktorom sa rušia súbory a pridávajú sa nové súbory, bol použitý model Turingovho stroja s dvomi páskami. Na zabezpečenie spojenia operácií na súboroch a ich stavov je potrebná existencia transformácie každého súboru do jedinečnej postupnosti. Dizertant toto spojenie formuluje definíciou 5.3.1. Následne definuje Turingov stroj pre požadované správanie.

Druhým hlavným prínosom dizertačnej práce je špecifikácia formálneho modelu pre implementáciu. S cieľom zjednodušenia procesu verifikácie je model implementácie definovaný rovnakým spôsobom ako je definovaný model požadovaného správania. Konečno stavový automat definuje správanie jedného špecifického súboru na mobilnom zariadení. Aby bolo možné zvládnuť všetky dostupné súbory, množstvo automatov je rovné počtu súborov. Turingov stroj definuje schopnosť modelovať neobmedzené množstvo súborov a správanie je definované konečno stavovým automatom, ktorý je opäť simulovaný Turingovým strojom.

Tretím hlavným prínosom dizertačnej práce je verifikačný model požadovaného správania. Formálny model požadovaného správania bol definovaný Turingovým strojom. Formálny model správania bol zapísaný prostriedkami verifikačného nástroja Uppaal a boli s ním

vykonané verifikačné experimenty. Experimety ukázali, že automaty sú v konzistentných stavoch, čo znamená, že obsahy chránených privátnych súborov zostanú na mobilnom zariadení.

V súvislosti s riešenou témou dizertant publikoval v rokoch 2015 a 2016 celkom 7 prác. Jedna práca bola publikovaná ako kapitola v knihe vydanej zahraničným vydavateľom, dva príspevky v časopisoch a 4 príspevky na medzinárodných konferenciách. V týchto prácach bola pojednávaná otázka bezpečnosti mobilných zariadení a dokumentovaný základný koncept dizertácie týkajúci sa dynamického mechanizmu oprávnení v operačnom systéme Android. Je na škodu, že dizertant nepublikoval návrh nového formálneho modelu riadenia prístupu k súborom na mobilnom zariadení, verifikáciu a implementáciu návrhu.

Na základe celkovej publikačnej činnosti dizertanta ako aj na základe predloženej dizertačnej práce možno konštatovať, že dizertant je pracovník s primeranou vedeckou erudíciou.

Predložená dizertačná práca dokumentuje nielen schopnosť dizertanta, že ovláda vedecké metódy práce a priniesol nové vedecké poznatky, ale aj schopnosť vykonávať vysoko odbornú inžiniersku prácu.

Otázky na dizertanta:

1. Aké dôvody viedli dizertanta pre špecifikáciu formálneho modelu pre implementáciu? Je formálny model požadovaného správania ekvivalentný formálnemu modelu pre implementáciu?
2. Mohol by dizertant uviesť aktuálny stav v publikačnej činnosti týkajúci sa jadra dizertácie?
3. Môže byť navrhnutý koncept zvýšenia bezpečnosti privátnych súborov na mobilnom zariadení použitý aj na zariadeniach s iným operačným systémom ako je Android?
4. Implementácia navrhnutej metódy predpokladá prebalenie (repackaging) aplikácií s cieľom monitorovať tok údajov (tainting). Je vždy možné prebalenie aplikácie a za akých podmienok?
5. Bola prototypová implementácia navrhnutej novej metódy riadenia prístupu podrobená reálnym testom, napríklad penetračným testom?

Celkové hodnotenie dizertačnej práce.
Dizertačnú prácu Ing. Lukáša Arona považujem za prínosnú pre aktuálnu problematiku zvýšenia bezpečnosti privátnych údajov na mobilných zariadeniach a práca zodpovedá všeobecne uznávaným požiadavkám pre udelenie akademického titulu.

V Bratislave, dňa 28.2.2018 podpis oponenta